计算机网络通信安全数据加密技术

摘　要：在当今网络信息快速发展的时代，网络通信已经遍布多个社会领域中，对于社会发展的推动和人们日常生活的便捷起到了重要的作用。计算机网络具有互联性、开放性、分布不均匀性等特点和在其它技术的缺陷，使网络通信安全的事件频繁发生，用户使用受到严重影响。对人们在网络活动上的保密性要求也越来越高，应用数据加密技术，保证了人们在网络活动中对自己的数据和一些相关资料保密的要求，保证了网络的安全性和保密性。

关键词：网络通信；数据加密

中图分类号：TJ768　　文献标识码：A

文章编号：1671-0134（2017）12-106-02　　DOI：10.19483/j.cnki.11-4653/n.2017.02.030

■文 / 白荣建

1. 计算机网络通信与数据加密的必要性

1.1 计算机网络通信

网络通信是用物理链路将每个独立的主机和工作站有效地连接在一起，形成多个网络间的数据链路，使其达成通信与资源共享的目的。网络的通信多数是说网络的协议，对信息沟通和会话构成连接，网络的协议是对代码传输、信息传输的速度与传输的步骤等指定的标准进行控制。

1.2 数据加密的必要性

数据安全的技术核心是数据加密技术，特别是在当今互联网正是高潮的时代，每个人每天都会用到互联网，资金、文件等重要信息都有可能受到危害。这让保护数据不被盗取、篡改、破坏等问题受到了人们极大的重视。而解决这些问题的技术关键就是数据加密技术。密钥是数据加密技术中必不可少的，有 20% 来自内部未授权的存取，而内部安全威胁超过了 80% 多，电子文件泄露占安全漏洞中造成的损害高达 30% 多，而防火墙这些常见的内网安全措施并不能有效地阻止公司机密信息的泄露。所以数据加密是非常重要的，不管是外部威胁还是内部威胁都可以有效地防范。

2. 密钥密码技术

密码学的起源可以追溯至古埃及的象形文字。密码学是研究如何通过编码技术来保证机密信息的安全性，它是由密码编码学和密码分析学两部分构成。一个密码系统通常可以完成信息的加密变换和解密变换。加密变换是采用一种编码算法将原有信息转换一种不可理解的编码，从而起到保护机密信息的作用。

解密变换则是与加密变换完全相反的过程，利用解密变换编码算法将不可理解的信息还原为原来的信息，但是解密要比加密困难得多。密码技术涉及密码设计、密码分析、密钥管理等内容。密码设计的目的是保证信息的机密性。基本手段是将信息加以伪装，使其在存储和传输过程中不会泄密。在多数的时候，数据加密技术分为对称加密技术和非对称加密技术。

3. 常见两种数据加密技术

3.1 对称数据加密

对称加密是最快速、最简单的一种加密方式，加密与解密用的是同样的密钥。密钥的大小要照顾到安全性和效率。对称数据加密技术有算法公开、加密速度块、计算量小、高效加密等特点。对称加密通常使用的是相对较小的密钥，一般小于 256 bit。因为密钥越大，加密越强，但加密与解密的过程越慢。如果只用 2 bit 来做这个密钥，那黑客们可以先试着用 0、1、2 来解密，但如果你的密钥有 1 MB 或者更大，黑客可能永远也无法破解，但解密和加密的过程要花费极为漫长的时间。

3.2 非对称数据加密

非对称加密给数据的加密与解密提供一个非常安全的方法，它是使用一对密钥，公钥和私钥。非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥，私钥只能由一方安全保管，不能对外泄漏，而公钥则可以发给任何有需求的人。非对称加密算法对机密信息交换实现的过程是：A 先生成一对密钥且将其中的一把密钥作为公用密钥向外公开；B 得到公开密钥使用该密钥对信息进行加密完成后再发给 A；A 再用自己独有的专用密钥对其加密后的机密信息进行解密，A 只能用独有密钥进行解密其公开的密钥进行加密后的任何信息。

4. 数据安全加密

4.1 链路加密

链路加密方法有时也叫作链路级或链路层加密，在网络通信链路上加密就是在信息传输前对数据进行加密处理，其实就是一个节点机经过所有的网络都进行加密和解密的

过程，而且每个节点机都必须有加密和解密的密码装置，才可以进行加密和解密。

数据整个传输过程中，数据每经过一个链路或者节点的时候都需要先解密然后再进行加密的步骤，在传输的过程中数据都是以密文编码的形式出现的，为了确保通信的安全性，数据不会显示出信息的接收和发出点信息，信息的频率和长度也是不显示出来的。

数据链路层是 OSI 系统结构中的第二层，每条链路对应不同的密钥，这样当一条链路上的密钥被破解也不会导致其他链路上的加密文件信息被破解出来。

4. 2 端到端加密方式

端到端加密方式中间节点不需要加密或者解密，只发送时加密信息，接收时解密信息，加密为了方便也可以用软件进行实现。

端到端的加密方式下，用户之间都会有一条虚拟的保密通道，密钥的总数和用户对的数目是一样的，且每对用户的密钥是共享的。身份认证方面来看，链路加密只能对节点的认证。如用节点 A 的密钥报文，仅可以保证它是来自节点 A，这其中也有可能是另一个用户路过节点 A。端对端加密方式对用户是可见的，所以可以看到文件的来源、谁发出的都很清晰。

多个用户两两通信的话，共需 n×（n-1）/2 种密钥，每个用户需（n-1）种。网上通信的用户增加密钥的数量也随之增加。为了使用安全，密钥需要每隔一段时间进行更换，有些密钥在特殊时候只能使用一次，这对密钥的用量非常大。

5. 数据加密技术在计算机网络通信中的应用

5. 1 数据加密技术在电子商务中的应用

目前电子商务蒸蒸日上，极大地促进了社会的进步，给人们的工作及生活提供了很大的便利条件。互联网设计的初衷只是为用户提供一种弹性的、快速的通讯平台，由于要确保电子商务的持续快速健康发展，电子商务中所涉及的电子交易需通过互联网进行，并不具备商业交易的安全性。

因此必须具备安全的计算机网络环境，其中最主要的表现即是网络中的交易信息安全，可以将 SET 安全协议、SSL、数字签名、证书等数据安全加密技术应用于电子商务活动中，从而有效实现交易双方的信息数据不被泄密与破坏。

5. 2 数据加密技术在计算机软件中的应用

随着计算机网络通信领域的不断发展，计算机软件也得到了极为快速的开发。如果杀毒软件在数据加密的过程中感染了病毒，那么程序或者数据是否有签名将无法得到检查，所以在对程序进行加密时，应该对需要加密或者解密的文件检查一下是否存在病毒。

许多黑客都是通过这些带有病毒的软件交互数据时进行信息的盗取，对用户使用造成严重的影响，所以对软件进行加密处理就非常重要了，用数据加密技术对应用程序软件进行加密，可以确保自身的数据不被盗取，预警系统也可以将出现的网络安全问题进行上报反馈，用户对其安全问题进行处理。

每位用户应该对应用软件进行定期的检查，以保证安全，对藏在程序深处的病毒要及时有效地处理，维护数据信息的安全。

5. 3 数据加密技术在局域网中的应用

现在许多行业为了提高工作效率和应用，都建立起自己内部的局域网，这就将大量的数据信息置于网络环境下，用于治疗的快速传输和一些重要事项的通知等，假如没有有效的防护措施，肯定会给公司和员工带来非常严重的风险。而数据加密技术在局域网中主要是通过路由器和发送者对数据信息进行技术加密，即确保了数据信息在局域网内传递的安全性，而且还能防御来自外部的攻击，这样就保证了公司内部重要信息不被盗取和破坏。

5. 4 数据加密技术应用于虚拟专用网络

现在大部分公司都搭建了自己私有的办公网络系统，由局域网实行单位内部数据的共享，然另一方面，分公司需要跨地区进行经营，所以需要租用一个专线来连接各个分公司的局域网来构成一个广域网实现共享数据的支持。现在已经有了加密解密功能的路由器，发送方发送的数据信息离开 vpn 时，路由器会对其信息进行加密，在传输过程中是以密文的方式，到目的地 LAN，路由器会对密文进行解密，接收用户就可以看到发送者发送的数据信息。既确保了数据的安全，传输方式又简易方便。

6. 结束语

计算机通信网络安全需要我们充分地重视，它是客观存在的，我们应该进一步地对通讯安全进行加强保护，对于目前来讲，计算机网络安全越来越受到重视，是信息安全备受关注的时候，黑客不断地在网络安全中出现，对个人信息造成泄密，现在计算机网络通信技术的应用广泛，给人们的生产和生活带来了较大的便利，这也是计算机网络通信安全数据加密技术在网络安全中的重要作用。

（作者单位：新华社技术局程控电话部）